Oleksii GAVRYLENKO[1], Yuliia KOZHEDUB[2], Serhii IVANCHENKO[3],
Yevhen PELESHOK[4], Nina CHALA[5]

Scientific supervisor: Alexander KORCHENKO[6]

PECULIARITIES OF APPLICATION OF HARMONIZED INTERNATIONAL STANDARDS FOR THE ESABLISHMENT OF INFORMATION PROTECTION SYSTEMS IN UKRAINE

Abstract: The basic stages of creating information security systems based on the provisions of national regulations are considered. The algorithm of construction of the information security system, which circulates in the information systems of the organization and the documents to be developed within the framework of their creation, is shown. The possibility of application of harmonized standards of the series DSTU ISO/IEC TR 13335 for ensuring the protection of information in accordance with the legislation of Ukraine has been studied.

Keywords: security systems, management, information, information systems, security plan, information security risks.

[1] PhD Eng (Mathematical modeling and computational methods), Associate Professor, IT-Security Academic Department, National Aviation University, gavrylav@gmail.com

[2] PhD Eng (Weapons and military equipment), Senior Research Fellow, Scientific and organizational department of the Scientific and Research Center, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" JuliaKozhedub@email.ua

[3] Dr Eng (Information security), Professor, Chief of the Scientific and Research Center, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" soivanch@ukr.net

[4] PhD Eng (Mathematical modeling and computational methods), Deputy Chief of the Scientific and Research Center, Institute of Special Communication and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" pel85@ukr.net

[5] Dr. Public Administration (Economic Policy), Professor, Departmens of Marketing and Business Management, Faculty of Economics, National University of Kyiv-Mohyla Academy, n.chala@ukma.edu.ua

[6] Dr Eng (Information security), Professor, Laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala (Akademia Techniczno-Hu-manistyczna, Bielsko-Biała, Poland), Leading Researcher of the National Academy of SS of Ukraine, icaocentre@nau.edu.ua

OSOBLIWOŚCI STOSOWANIA ZHARMONIZOWANYCH MIĘDZYNARODOWYCH STANDARDÓW DO USTALENIA SYSTEMÓW OCHRONY INFORMACJI NA UKRAINIE

Streszczenie: Rozważane są podstawowe etapy tworzenia systemów bezpieczeństwa informacji w oparciu o przepisy krajowych przepisów. Pokazany jest algorytm budowy systemu bezpieczeństwa informacji, który krąży w systemach informatycznych organizacji oraz dokumenty opracowywane w ramach ich tworzenia. Zbadano możliwość zastosowania zharmonizowanych norm serii DSTU ISO/IEC TR 13335 w celu zapewnienia ochrony informacji zgodnie z ustawodawstwem Ukrainy.

Słowa kluczowe: systemy bezpieczeństwa, zarządzanie, informacja, systemy informacyjne, plan bezpieczeństwa, zagrożenia bezpieczeństwa informacji

1. Introduction

Organizations of different levels of subordination and ownership, from governmental to commercial, accumulate information in information systems that reflect their activities. Loss of confidentiality, integrity, availability of information can impair the proper functioning of any organization. Therefore, information security and management of information systems security in organizations are the main problems, and the necessity to create information security systems is a particularly pressing issue today.

2. Basic studies

In accordance with the requirements of the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" [1], information, the protection requirements of which are established by law, must be processed in information systems using a comprehensive system of information protection with confirmed compliance. The procedure for establishing such protection systems is defined in the RD TPI 3.7-003-2005 [2] (regulatory document on technical protection of information) and in order to confirm their compliance with the requirements of the legislation, organizations must follow the established procedure.
However, in Ukraine, the creation of security systems can be carried out according to harmonized international standards: DSTU ISO/IEC 27k (Information Security Management Systems), DSTU ISO/IEC TR 13335 (all five parts of this series are valid in Ukraine. In this work, consider the provisions DSTU ISO/IEC TR 13335-2: 2003 [3]), which are not mandatory documents. Therefore, it makes sense to find out whether the recommendations of these international standards can be used to provide protection in systems that process information that needs protection under Ukrainian law.

Any activity should be subject to a certain sequence of actions, especially if it is related to such important tasks as protecting information and managing the security of organizations' information systems.

Organizational and technical provisions for ensuring the technical protection of information are determined by DSTU 3396.0-96 [4], according to which such protection is performed in stages:

1) identification and analysis of threats;
2) development of information security system;
3) implementation of the information security plan;
4) control of the functioning and management of the information security system.

Based on this standard [2], was developed, which contains the following measures:

1) the formation of general requirements for the security system (justification of the need to create, survey environments, formulation of the task of protection, in particular, risk analysis and identification of threats);
2) development of information security policy in the information system (object study and threat analysis on which the system is created, choice of security system, policy design and choice of solutions to counter threats);
3) development of the technical task for creation of the protection system;
4) development of the project of protection system (sketch, technical, working project, including, selection and development of means of protection);
5) putting in place a security system and evaluating the security of information in the information system (preparation for deployment, creation of a security service and completion of a security plan, manning security, user training, construction and commissioning, preliminary testing, pilot operation, evaluation compliance);
6) maintenance of the security system (organizational support of operation, management of protection means in accordance with the protection plan and operational documentation).

The application [3] provides the following.

Goals (to be achieved), strategies (how to achieve these goals – information security policy) and techniques (rules to achieve the goals – policies) can be defined for each level of organization and for each structural unit. However, in order to achieve the effectiveness of information systems security, it is necessary to streamline different goals, strategies and techniques for each organizational level and unit. Consistency between the relevant documents is very important, as most threats (such as system crashes, file destruction, and fire) are common problems for the organization's continuity.

Differences in management types, sizes and structures of organizations cause the orientation of the process to the external and internal environment, which will be covered by the protection system.

The starting point for creating a security system is to set clear goals for protecting the organization's information system. These goals go beyond those of a higher level (for example, the exercise of authority in accordance with a legal act or business plan) and, in turn, define the information security policy of the organization and partial security policies, the latter detailing at the executive level the provisions of the information security policy of the organization. The advantages of this approach are: integrated security, interoperability, consistency, mobility, efficiency, interaction between organizations.

In some situations, the organization resolves issues regarding the use of protection or suspension at some stage. Such decision should be made only after the management of the organization carefully analyzes all potential risks and adverse situations, probability of occurrence of events, incidents of information security.

An important document is an information system security plan – a document that defines the concerted steps that must be taken to implement the organization's information security policies. This plan should include short, medium and long-term priority measures with appropriate investment, funding terms, cost of operation, loads, etc., as well as a timetable for implementation.

All information security measures will be most effective if they are applied simultaneously across the organization. The process of protecting information systems is an important separate activity cycle that must be integrated into all stages of the information system life cycle.

The fulfillment of such tasks is entrusted to the information security services created by the organizations, which circulate information that needs protection under the legislation of Ukraine. To maximize the effectiveness of information security services, their composition should include specialists with basic security training and technical aspects of the information system.

Information systems security management is the process of achieving and maintaining the required levels of confidentiality, integrity, and accessibility of information circulating in an organization's information systems. Information security management functions include:

1. defining the goals, strategies (information security policy) and techniques (partial information security policies) during the security organization;
2. determining the necessary conditions for the organization of protection;
3. identification and analysis of information security risks for all information assets in the organization;
4. identification of appropriate remedies;
5. control over the application and functioning of the security measures necessary for the effective protection of information and the normal operation of the organization;
6. development and implementation of the program of competence in defense;
7. detection and response to information security incidents.

Also in [3] recommendations on protection of information in the information system are given concerning: selection and conformity of means of protection in the information system, consideration of risks, methods and plan of protection, implementation of means of protection, competence in protection, control, servicing, mechanisms of refining, processing of incidents of information. security.

3. Conclusions

Finally, comparison of stages [4], activities [2], functions and recommendations [3] shows that their main content is relevant in the first place to the organizational aspect of system creation. The exception are the issues of incident management, as well as the risk management processes, which in [2] and [4] are not given the necessary attention and which are perspective directions of improvement of the relevant regulatory framework. It should be noted that risk management and incident management in international regulations are crucial issues for the creation and effective functioning of security systems.

Therefore, it has been found that the basic measures for the creation of security systems according to [3] are consistent with the measures provided for in [4] and [2]. Therefore, we can assume that security systems, built in accordance with the guidelines of the series DSTU ISO/IEC TR 13335, will also meet the requirements of the normative documents of Ukraine regarding the suitability for processing information that needs protection in accordance with its legislation. This is true in the case of their use in the formulation of requirements for protection systems of the generally accepted criteria for assessing the security of information in information systems against unauthorized access, which are not considered in relation to the measures [3].
The experience of globally recognized organizations that offer best practice, time-tested, should, in our opinion, be transferred to Ukrainian soil.

REFERENCES

1. Information protection in information and telecommunication systems. Law of Ukraine. Valid, in the wording of Law No. 1170-VII of March 27, 2014. – The Official Bulletin of the Verkhovna Rada of Ukraine, 1994, No. 31, Art. 286.

2. The order of carrying out works on creation of the complex system of information protection in the information and telecommunication system. RD TPI 3.7-003-2005. Approved by the order of the SSSCIP of the Security Service of Ukraine of November 8, 2005, No. 125, as Amended in accordance with the Order of the State Security Service Administration of December 28, 2012, No. 806.

3. Information Protection. Technical protection of information. Basic principles. DSTU 3396.0-96. National standard of Ukraine. Valid from January 1, 1997. Approved and enforced by the Order of the State Consumer Standard of Ukraine from October 11, 1996 No. 423. – State Consumer Standard of Ukraine, 1996. – 10 p.

4. Information technology. Guidelines for the management of IT Security. Part 2: Managing and planning IT security. DSTU ISO/IEC TR 13335-2: 2003 (ISO/IEC TR 13335-2: 1997, IDT). National standard of Ukraine. Valid from January 1,

2005. Approved by the Order of the State Consumer Standard of Ukraine from October 31, 2003 No. 189. – State Consumer Standard of Ukraine, 2004. – 20 p.